APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/635,882	08/05/2003	Alpesh Patel	CISCP334/6994	1592

22434   7590   02/05/2008
BEYER WEAVER LLP
P.O. BOX 70250
OAKLAND, CA 94612-0250

EXAMINER
HOFFMAN, BRANDON S

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
02/05/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

<table>
<tr><td rowspan="2">Office Action Summary</td><td>Application No.
10/635,882</td><td>Applicant(s)
PATEL ET AL.</td><td></td></tr>
<tr><td>Examiner
Brandon S. Hoffman</td><td>Art Unit
2136</td><td></td></tr>
</table>

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 November 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4,6-31 and 33-55* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,6-31 and 33-55* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date *11-15-07*.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1.   Claims 1-4, 6-31, and 33-55 are pending in this office action, claim 55 is newly

added.

Continued Examination Under 37 CFR 1.114

2.   A request for continued examination under 37 CFR 1.114, including the fee set

forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this

application is eligible for continued examination under 37 CFR 1.114, and the fee set

forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action

has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on

November 15, 2007, has been entered.

3.   Applicant's arguments, filed November 15, 2007, are moot in view of the new

ground of rejection.

Information Disclosure Statement

4.   The information disclosure statement (IDS) submitted on November 15, 2007, is

in compliance with the provisions of 37 CFR 1.97. Accordingly, the information

disclosure statements are being considered by the examiner.

Claim Rejections - 35 USC § 102

5.   Claims 1-4, 6-31, and 33-55 are rejected under 35 U.S.C. 102(e) as being

anticipated by Malinen et al. (U.S. Patent Pub. No. 2003/0028763).

Regarding claims 1 and 45-47, Malinen et al. teaches in a server adapted for

authentication, authorization, and accounting, a method/computer-readable

medium/server for generating a shared key between a Home Agent and a Mobile node,

comprising:

- Receiving a request message from a Home Agent, the request message

  identifying the Mobile Node (fig. 2, step 215);

- Deriving key information from a key or password associated with the Mobile

  Node (paragraph 0180); and

- Sending a reply message to the Home Agent, the reply message including the

  key information associated with the Mobile Node, thereby enabling the Home

  Agent to derive a shared key to be shared between the Mobile Node and the

  Home Agent from the key information, wherein the reply message does not

  include the shared key to be shared between the Mobile Node and the Home

  Agent **in any form** (fig. 2, ref. step 230-240 and paragraph 0181-0183 and

  paragraph 0086).

Regarding claim 2, Malinen et al. teaches wherein deriving key information

comprises deriving the key information from a second set of key information derived

from the key or password (paragraph 0180, there are two parts to the ID).

Regarding <u>claim 3</u>, <u>Malinen et al.</u> teaches wherein deriving key information comprises obtaining the derived key information from a domain controller or server (fig. 2, AAAL is the AAA server).

Regarding <u>claim 4</u>, <u>Malinen et al.</u> teaches wherein the request message is an access request message and the reply message is an access reply message (fig. 2, AR/LA is an access router).

Regarding <u>claim 5</u>, <u>Malinen et al.</u> teaches wherein the key or password comprises a Windows password associated with the Mobile Node (paragraph 0010, the mobile node is a mobile device with a processor, known to use passwords).

Regarding <u>claim 6</u>, <u>Malinen et al.</u> teaches further comprising obtaining the key or password from a domain controller (fig. 2, AGW/AAAH).

Regarding <u>claim 7</u>, <u>Malinen et al.</u> teaches wherein obtaining the key or password from the domain controller comprises:

- Sending a request to the domain controller for the key or password associated with the Mobile Node; and receiving the key or password associated with the Mobile Node from the domain controller (fig. 2, step 225).

Regarding claim 8, Malinen et al. teaches further comprising applying the key

information to authenticate the request message (paragraph 0182).

Regarding claim 9, Malinen et al. teaches wherein the key or password is stored

at the Mobile Node, thereby enabling the Mobile Node to derive the key information

from the key of password (paragraph 0183).

Regarding claims 10 and 48-50, Malinen et al. teaches in a Home Agent

supporting Mobile IP, a method/computer-readable medium/Home Agent of

authenticating a Mobile Node, comprising:

- Receiving a Mobile IP registration request from a Mobile Node, the Mobile IP

  registration request identifying the Mobile Node (fig. 2, step 215);

- Sending a request message to a AAA server, the request message identifying

  the Mobile Node (fig. 2, step 225);

- Receiving a reply message from the AAA server, the reply message including

  key information associated with the Mobile Node (paragraph 0180);

- Deriving a key from the key information, the key being a shared key between the

  Mobile Node and the Home Agent, **wherein deriving the key from the key**

  information does not include decryption of the key information (fig. 2, ref.

  step 230-240 and paragraph 0181-0183); and

- Sending a Mobile IP registration reply to the Mobile Node, wherein the Mobile IP

  registration reply does not include the key **in any form** (fig. 2, step 245 and

  paragraph 0086).

Regarding <u>claim 11</u>, <u>Malinen et al.</u> teaches wherein the Mobile IP registration

request includes a CHAP challenge and response (fig. 2, step 205 and 210).

Regarding <u>claim 12</u>, <u>Malinen et al.</u> teaches wherein deriving a key from the key

information comprises deriving the key from the key information and a CHAP challenge

and response obtained from the Mobile IP registration request (paragraph 0180).

Regarding <u>claim 13</u>, <u>Malinen et al.</u> teaches wherein deriving the key and sending

the Mobile IP registration reply to the Mobile Node are performed when the reply

message received from the AAA server indicates that the Mobile Node is successfully

authenticated (fig. 2, step 215 and 220).

Regarding <u>claim 14</u>, <u>Malinen et al.</u> teaches wherein the request message is an

access request message and the reply message is an access reply message (fig. 2,

AR/LA is an access router).

Regarding <u>claim 15</u>, <u>Malinen et al.</u> teaches wherein the Mobile Node is to derive the shared key from a second set of key information stored at the Mobile Node (paragraph 0180, there are two parts to the ID).

Regarding <u>claim 16</u>, <u>Malinen et al.</u> teaches wherein the key information is equivalent to the second set of key information (paragraph 0180, there are two parts to the ID).

Regarding <u>claim 17</u>, <u>Malinen et al.</u> teaches wherein the second set of key information stored at the Mobile Node is a root key, a password, or a key shared between the Mobile Node and the Home Agent in a previous session (paragraph 0184).

Regarding <u>claims 18 and 39</u>, <u>Malinen et al.</u> teaches wherein the registration request includes a SPI, replay protection timestamp, and indicates an algorithm to be used to authenticate the registration request, wherein the SPI, the replay protection timestamp, and the algorithm are associated with the key information (fig. 2, step 215, RPI).

Regarding <u>claim 19</u>, <u>Malinen et al.</u> teaches further comprising installing the derived key, the SPI, the replay protection timestamp, and the algorithm in a security association (paragraph 0161).

Regarding <u>claims 20 and 40</u>, <u>Malinen et al.</u> teaches wherein the registration reply includes a SPI, replay protection timestamp, and indicates an algorithm to be used to authenticate the registration replay, wherein the SPI, the replay protection timestamp, and the algorithm are associated with the key information (fig. 2, step 280, RPI).

Regarding <u>claim 21</u>, <u>Malinen et al.</u> teaches wherein the Mobile IP registration reply indicates that the Mobile Node is to derive the shared key between the Mobile Node and the Home Agent (paragraph 0155-0161).

Regarding <u>claims 22 and 42</u>, <u>Malinen et al.</u> teaches wherein at least one of the presence of one or more extensions in the Mobile IP registration reply and an SPI in the Mobile IP registration reply indicates that the Mobile Node is to derive the shared key between the Mobile Node and the Home Agent (paragraph 0155-0161).

Regarding <u>claims 23 and 43</u>, <u>Malinen et al.</u> teaches wherein the Mobile IP registration request indicates that the Home Agent is to derive the shared key between the Mobile Node and the Home Agent from a second set of key information received by the Home Agent (paragraph 0155-0161).

Regarding <u>claims 24 and 44</u>, <u>Malinen et al.</u> teaches wherein at least one of the presence of one or more extensions in the Mobile IP registration request and an SPI in

the Mobile IP registration request indicates that the Home Agent is to derive the shared

key between the Mobile Node and the Home Agent (paragraph 0155-0161).

Regarding claim 25, Malinen et al. teaches wherein the presence of an

authentication protocol extension in the Mobile IP registration request indicates a

protocol to be used to authenticate the Mobile IP registration request and derive the

shared key (paragraph 0155-0161).

Regarding claim 26, Malinen et al. teaches wherein the presence of a session

key extension and derived session key extension in the registration request indicates

that both a session key and a derived session key are to be generated and installed

(paragraph 0155-0161).

Regarding claim 27, Malinen et al. teaches further comprising receiving a

subsequent Mobile IP registration request from the Mobile Node to refresh the derived

session key (paragraph 0155-0161).

Regarding claim 28, Malinen et al. teaches further comprising authenticating the

subsequent Mobile IP registration request using the session key (fig. 2, step 270).

Regarding claim 29, Malinen et al. teaches further comprising sending a

subsequent Mobile IP registration reply to the Mobile Node including the derived

session key extension, wherein the Mobile IP registration reply is to be authenticated by

the Mobile Node using the session key (fig. 2, step 245-280).

Regarding claim 30, Malinen et al. teaches wherein the key information is a

previously used session key shared between the Mobile Node and the Home Agent

(paragraph 0163).

Regarding claim 31, Malinen et al. teaches wherein the key information is derived

from a password associated with the Mobile Node (paragraph 0010, the mobile node is

a mobile device with a processor, known to use passwords).

Regarding claim 32, Malinen et al. teaches wherein the password is a Windows

password (paragraph 0010, the mobile node is a mobile device with a processor, known

to use passwords).

Regarding claim 33, Malinen et al. teaches further comprising deriving a

subsequent key from the shared key (paragraph 0186).

Regarding claim 34, Malinen et al. teaches wherein deriving the subsequent key

from the shared key is performed when a binding associated with the Mobile Node is

cleared (paragraph 0035).

Regarding <u>claim 35</u>, <u>Malinen et al.</u> teaches wherein the binding associated with the Mobile Node is cleared upon expiration of the lifetime of the Mobile Node or deregistration of the Mobile Node (paragraph 0034-0035).

Regarding <u>claims 36 and 51-53</u>, <u>Malinen et al.</u> teaches in a Mobile Node, a method/computer-readable medium/mobile node of registering with a Home Agent supporting Mobile IP, comprising:

- Sending a registration request to the Home Agent (fig. 2, step 215);

- Receiving a registration reply from the Home Agent, the registration reply indicating that the Mobile Node is to derive a key to be shared between the Mobile Node and the Home Agent, wherein the registration reply does not include the key to be shared between the Mobile Node and the Home Agent **in any form** (paragraph 0180); and

- Deriving a key to be shared between the Mobile Node and the Home Agent from the key information stored at the Mobile Node, **wherein deriving the key from the key information does not include decryption of the key information** (fig. 2, ref. step 230-240 and paragraph 0181-0183 and paragraph 0086).

Regarding <u>claim 37</u>, <u>Malinen et al.</u> teaches wherein deriving a key from the key information comprises deriving the key from the information and a CHAP challenge and response obtained from the registration reply (fig. 2, step 205-215).

Regarding <u>claim 38</u>, <u>Malinen et al.</u> teaches wherein the key information is a root key, a password, or a key shared between the Mobile Node and the Home Agent in a previous session (paragraph 0008).

Regarding <u>claim 41</u>, <u>Malinen et al.</u> teaches wherein the registration reply indicates whether the Mobile Node is to derive the shared key between the Mobile Node and the Home Agent, the method further comprising:

* Determining from the registration reply whether the Mobile Node is to derive the key; wherein deriving a key is performed when it is determined from the registration reply that the Mobile Node is to derive the key (paragraph 0178).

Regarding <u>claim 54</u>, <u>Malinen et al.</u> teaches wherein deriving key information from a key or password associated with the Mobile Node includes deriving the key information from a password, wherein the key information is not derived from a key (paragraph 0009).

Regarding <u>claim 55</u>, <u>Malinen et al.</u> teaches the reply message does not include the shared key to be shared between the Mobile Node and the Home Agent in an encrypted form or a decrypted form (fig. 2, step 240, create the GK_M).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Brandon Hoffman/

BH